UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/937,415 | 11/15/2001 | Frank Muller | PTT-124 (402562US) | 9606 |

7265      7590      03/07/2005

MICHAELSON AND WALLACE
PARKWAY 109 OFFICE CENTER
328 NEWMAN SPRINGS RD
P O BOX 8489
RED BANK, NJ  07701

| EXAMINER |
|---|
| CHAI, LONGBIT |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on <u>*15 November 2001*</u>.

2a)☐ This action is **FINAL.**     2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-17* is/are pending in the application.

    4a) Of the above claim(s) *1-8* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage

        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *9/26/2001*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

## DETAILED ACTION

### *Preliminary Amendment*

1.      Claims 1 – 8 have been canceled; new claims 9 – 17 have been added in a

preliminary amendment filed 9/26/2001.

### *Priority*

2.      Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d)

is acknowledged.

The application is filed on 11/15/2001 but has a foreign priority application

filed on 4/1/1999.

### *Specification*

3.      The abstract of the disclosure is objected to because the notations such as

"input symbol (5, 20)" and "function (2)" are not clearly defined before the use.

Correction is required for all of the related issues in the abstract and specification.

See MPEP § 608.01(b).

4.      The string of modification characters shown on TABLE II ROW (Step n = 6)

should be "5 5 6 3 4" instead of "5 5 6 3 5" because of (7+5) mod 8 = 4.

Appropriate correction is required. See 37 CFR 1.71.

### Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5.     Claim 9 is rejected under 35 U.S.C. 101 because the claimed subject matter is not technologically embodied which is just an abstract idea. It is suggested by the Examiner to incorporate the limitations by being embodied on a computer readable medium. Any other claims not addressed are rejected by virtue of their dependency.

### Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6.     Claim 9 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

This is because a typical embodiment of any authentication system would include both enciphering and deciphering sections. However, the deciphering mechanism is not clearly and specifically addressed in the specification. One

skilled in the art clearly would not know how to use the claimed invention to complete the entire process of the transmitted and received message for authentication purpose.

Any other claims not addressed are rejected by virtue of their dependency should also be corrected.


### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7.    Claims 9 – 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Ritter (Patent Number: 4979832), hereinafter referred to as Ritter.


As per claim 9, Ritter teaches a method for authentication of a string of input characters by means of an enciphering function enabled for enciphering said string of input characters under control of a string of key characters, comprising the steps of:

modifying, by application of a modification function, under control of a string of modification characters, said enciphering function (Ritter: see for example, Figure 1 Element 18 & 20, Column 5 Line 50 – 53 and Column 6 Line 17 – 20: The

CHANGES CONTROLLER as taught by Ritter is qualified to perform the

modification function);

enciphering, by application of an enciphering function, under control of said

string of key characters, said string of input characters (Ritter: see for example,

Figure 1 Element 12, 14 & 16, Column 5 Line 50 – 53 and Column 6 Line 8 – 16:

The COMBINER / SUBSTITUTE as taught by Ritter is to perform the enciphering

function and Pseudo-Random number can serve as a KEY), characterized in that

said modification function is applied initially, prior to said application of the

enciphering function (Ritter: see for example, Figure 1 Element 18 & 20 and

Column 6 Line 21 – 24); and

said initially applied modification function modifies the enciphering function

under control of modification characters which are derived from said string of input

characters (Ritter: see for example, Figure 1 Element 10 & 18 and Column 6 Line

17 – 24).


As per claim 10, Ritter teaches the claimed invention as described above

(see claim 9). Ritter further teaches characterized in that said modification

characters are also derived from said string of key characters (Ritter: see for

example, Figure 1 Element 16, Column 5 Line 50 – 53 and Column 6 Line 8 – 16:

The Pseudo-Random number can serve as a KEY).

As per claim 11 and 17, Ritter teaches the claimed invention as described above (see claim 9 and 10 respectively). Ritter further teaches the modification function comprises the replacement of a character of the string of modification characters, by a replacement character obtained by an addition of two or more characters of the string of modification characters modulo the number of possible different characters (Ritter: see for example, Column 2 Line 16 – 18 and Column 2 Line 23 – 25: Examiner notes since the replacement character resulted from the combination / addition of two or more different characters must be coming from the predefined set of characters (i.e., S-Box or the substitution table), the modulo of addition with the size of S-Box or the substitution table must be utilized accordingly).

As per claim 12, Ritter teaches the claimed invention as described above (see claim 9). Ritter further teaches characterized in that the modification function comprises the modification of sequence numbers of two or more of the characters of the string of modification characters (Ritter: see for example, Figure 1 Element 10 &16, Column 6 Line 20 – 24 and Column 11 Line 7 – 12).

As per claim 13, Ritter teaches the claimed invention as described above (see claim 9). Ritter further teaches characterized in that, for the modification of the function, there is used as an initial function the function which was used earlier

for determining an earlier string of output characters (Ritter: see for example,

Figure 1 Element 18 & 20 and Column 6 Line 21 – 24).


As per claim 14, Ritter teaches the claimed invention as described above

(see claim 9). Ritter further teaches characterized in that the function is a

substitution function (Ritter: see for example, Column 6 Line 20 – 24).


As per claim 15, Ritter teaches the claimed invention as described above

(see claim 9). Ritter further teaches characterized in that the function is a

non-invertible function (Ritter: see for example, Abstract 4th Paragraph Line 4 – 5).


As per claim 16, Ritter teaches the claimed invention as described above

(see claim 9). Ritter further teaches characterized in that the function comprises a

substitution box containing replacement characters for the characters of the string

of input characters, and the modification function containing the exchange,

depending on the string of modification characters, of two or more characters of

the substitute box (Ritter: see for example, Figure 1 and Column 6 Line 1 – 35:

The "operation on a single block of data" as taught by Ritter is qualified as the S-

Box).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.
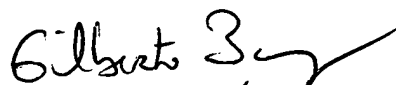
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit  Chai
Examiner
Art Unit 2131

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100